Celah Keamanan Sistem Autentikasi *Wireless* Berbasis *RADIUS*

Yesi Novaria Kunang
Program Studi Sistem Informasi
Universitas Bina Darma
Palembang, Indonesia
yesi_kunang@mail.binadarma.ac.id

Taqrim Ibadi
Program Studi Teknik Informatika
Universitas Bina Darma
Palembang, Indonesia
Taqrimibadi91@yahoo.com

Suryayusra
Program Studi Teknik Informatika
Universitas Bina Darma
Palembang, Indonesia
suryayusra@mail.binadarma.ac.id

***Abstrak*—Penggunaan teknologi jaringan berbasis *wireless* (tanpa kabel) memiliki resiko yang besar akan bahaya serangan dan pencurian informasi. Salah satu teknik pengamanan yang banyak digunakan pada jaringan *wireless* adalah system autentikasi yang menggunakan *RADIUS*. Untuk itu pada penelitian ini membahas pengujian penetrasi pada sistem Autentikasi *Wireless* berbasis *RADIUS* dengan tujuan untuk mencari celah keamanan pada sistem autentikasi berbasis *RADIUS*. Hasil yang didapatkan dari penelitian ini memperlihatkan bahwa Sistem autentikasi wireless berbasis *RADIUS* masih memiliki beberapa celah keamanan antara lain kemungkinan serangan *DoS* ke *Access point*, pencurian data *client* menggunakan *session hijacking*, dan pemutusan koneksi *client* untuk mengambil alih sesi koneksi. Rekomendasi dari penelitian ini diharapkan bisa menjadi acuan bagi administrator dan pengembang jaringan untuk menutup celah keamanan yang bisa dieksploitasi tersebut.**

Kata kunci—Pengamanan wireless; RADIUS; Session Hijacking; wireles; Sistem Autentikasi

I. PENDAHULUAN

Dengan makin berkembangnya teknologi mobile dengan hadirnya perangkat *notebook, tablet*, dan telepon seluller (*handphone*) mendorong makin pesatnya penggunaan jaringan *wireless* (tanpa kabel). Perangkat mobile tersebut mendominasi pemakaian teknologi *wireless*. Pemakaian jaringan *wireless* di sekolah, hotel, rumah sakit, *cafe* dan tempat umum lainnya bisa dijumpai di mana saja. Seseorang bisa terkoneksi melalui sebuah jaringan *wireless*, kapanpun dan dimananpun selagi terdapat jaringan *wireless*.

Dengan makin meluasnya penggunaan teknologi *wireless* tersebut, masalah terbesar adalah pada keamanan jaringan *wireless* itu sendiri. Beberapa riset telah membahas berbagai sistem pengamanan jaringan *wireless*, mulai dari pengamanan *access point* dengan menerapkan konsep *MAC Filtering*, menggunakan kunci pengamanan *WEP, WPA-PSK, WPA2-PSK*, serta sistem yang menggunakan autentikasi *captive portal*, *RADIUS* dan lainnya. Masing-masing teknologi tersebut memiliki kelemahan dan kelebihan masing-masing [1,10].

Kejahatan dunia maya (*cyber*) sudah begitu marak di kalangan masyarakat, terutama kejahatan yang memanfaatkan celah keamanan jaringan. Celah keamanan jaringan yang sering dimanfaatkan antara lain: *Sniffing to Eavesdrop* yang merupakan tindakan kejahatan yang siapapun bisa melakukannya dengan bantuan *software* yang banyak tersedia. Selain itu *IP Spoofing* dan *Session Hijacking* merupakan kejahatan yang cukup berbahaya yang bisa dieksploitasi untuk pencurian informasi. Teknik *Denial of Service Attack (DOS)* bisa mengganggu layanan di jaringan maupun layanan server, selain itu *Man in the Middle Attack* dimana penyerang menempatkan dirinya di antara komunikasi dua *host*, biasanya *server* dan *client* sehingga penyerang bisa mencuri informasi. Berdasarkan data statistik terbaru dari Pusat Layanan Informasi Keamanan internet Nasional, ID-SIRTII September 2012 dan Oktober 2012, tingkat kejahatan dari hari ke hari semakin meningkat. Dari data tersebut jenis kejahatan *SQL* masih menduduki peringkat pertama, disusul *BOTNET-CNC* dan kejahatan lainnya [3]

Untuk mengantisipasi hal-hal yang dapat mengancam data dan sistem jaringan, berbagai utilitas program dan teknik pengamanan telah dikembangkan. Mulai dari mempekerjakan administrator jaringan yang berpengalaman, menggunakan mekanisme sistem autentikasi terbaru dalam jaringan (*advanced authentication mechanism*), menggunakan teknik enkripsi setiap melakukan transfer atau komunikasi data, menginstalasi *firewall* pada jaringan *wireless* untuk melindungi *proxy server* adalah usaha-usaha yang dapat dilakukan untukpengamanan jaringan.

Teknologi sistem autentikasi *wireless* menjadi pilihan untuk pengamanan sistem *wireless* dengan jumlah *client* yang banyak dan adanya kesulitan pendistribusian *key* [10]. Sistem autentikasi yang paling banyak digunakan saat ini terutama di hotel-hotel, sekolah dan lain-lain yang memiliki jumlah *client* yang besar, sebagian besar berbasis *RADIUS*. Untuk itu pada penelitian ini membahas pengujian penetrasi pada sistem Autentikasi *Wireless* berbasis *RADIUS* dengan tujuan untuk mencari celah keamanan pada sistem autentikasi berbasis *RADIUS*. Hasil dari penelitian ini diharapkan bisa menjadi acuan bagi pengembang jaringan untuk menutup celah keamanan yang bisa dieksploitasi tersebut.

II. METODE PENELITIAN

Penelitian ini merupakan *Action Research*, yang bertujuan mengembangkan metode kerja yang paling efisien. Penelitian tindakan yang mendeskripsikan, menginterpretasikan dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau interversi dengan tujuan perbaikan atau partisipasi.[7,9]. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini,

a) Diagnosing;. Peneliti melakukan diagnosa terhadap sistem keamanan jaringan *wireless* berbasis *RADIUS*.

b) Action Planning: peneliti melakukan rencana tindakan yang akan dilakukan pada jaringan *wireless RADIUS* dengan membuat perancangan dan pengujian sistem keamanan jaringan.

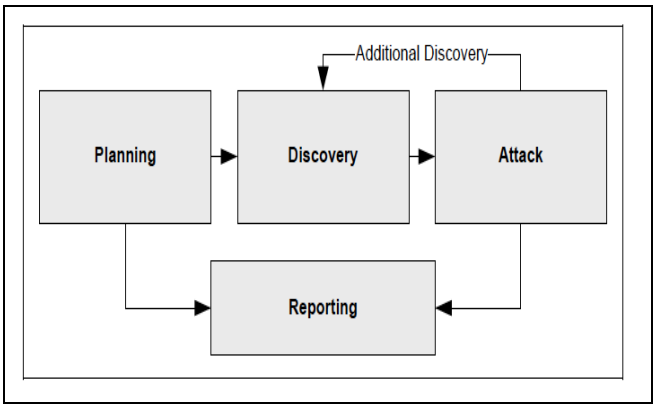
c) Action Taking : Peneliti mengimpelementasikan rencana dengan tindakan yang telah dibuat dengan menjalankan tahapan-tahapan mengikuti fase Penetrasi testing terhadap jaringan *wireless RADIUS* untuk mencari kelemahan sistem jaringan *wireless.*

d) Evaluating: Peneliti melaksanakan evaluasi hasil dari hasil penetrasi tadi yang menemukan celah keamanan sistem autentikasi *wireless* berbasis *RADIUS*, dalam tahap ini yang dilihat adalah apakah sistem keamanan jaringan *wireless RADIUS* berjalan dengan baik dan sesuai dengan rencana.

e) Specifying Learning: Melakukan review tahapan-tahapan yang telah berakhir dan mempelajari kriteria celah keamanan dan cara menutup celah keamanan tersebut.

Untuk pengujian celah keamanan sistem Autentikasi *wireless* pada penelitian ini menerapkan pengujian *White Box Testing* yang meperhitungkan mekanisme internal dari sebuah sistem atau komponen. *Penetration testing* yang dilakukan terhadap sistem atau jaringan dengan tipe *white box* ini, biasanya informasi-informasi mengenai sistem atau jaringan sudah diketahui. Tetapi hal tersebut tidak serta-merta memberikan kemudahan dalam melakukan penetrasi, hal tersebut tergantung dari penguji yang melakukan pengujian menilai sejauh mana kelemahan-kelemahan yang terdapat di dalam sistem atau jaringan [8].

Selain menggunakana metode penelitian pengujian *White Box*, penelitian ini juga mengacu pada dokumen *Guideline* untuk Pengujian *Information Security* yang dikeluarkan *United States National Institute of Standards and Technology (NIST)*, [6]. Pada rujukan tersebut untuk melakukan Fase Penetrasi Testing terdiri dari empat fase yang mencakup *Planning*, *Discovery, Attack* dan *Reporting*.

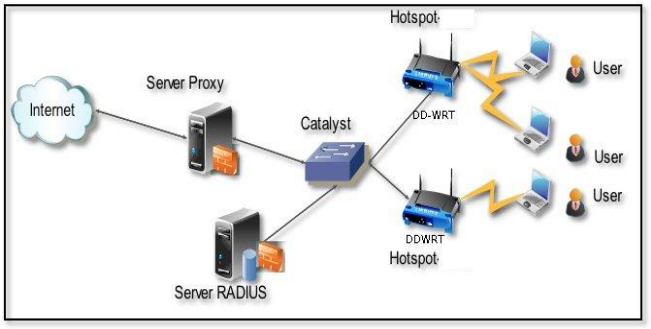


Gambar 1. Empat Fase Metodology Penetrasi Testing

III. FASE PENGUJIAN PENETRASI SISTEM

A. *Planning*

Di dalam penelitian ini akan dilakukan pengujian eksternal dan internal. Pada pengujian eksternal dilakukan penetrasi sebelum proses autentikasi *wireless* dengan tujuan mencari celah keamanan yang bisa dieksplorasi penyerang yang tidak memiliki akses login. Sedangkan pengujian internal dilakukan untuk mencari celah keamanan yang bisa dieksplorasi oleh pengguna setelah melakukan proses autentikasi *wireless*. Untuk pengujian secara eksternal dan internal tersebut juga dilakukan serangan yang bersifat pasif dan yang bersifat aktif. Untuk serangan pasif berupa serangan yang tidak mempengaruhi kerja sistem ataupun *resource* yang dimiliki sistem. Sedangkan serangan aktif yang dilakukan akan mempengaruhi /mengganggu kerja sistem dan *resource* sistem.



Gambar 2. Topologi Sistem Autentikasi *Wireless* yang diuji

Pada pengujian sistem autetikasi ini dilakukan pada sistem autentikasi *wireless* berbasis *RADIUS* yang menggunakan *tool freeradius* pada *server Ubuntu*, untuk sistem *redirect* autentikator digunakan *tools chillispot* pada *firmware DDWRT v24-sp2* yang ditanam pada *Access Point* jenis *WRT54GL v1.1*. Pada *access point firewall* tidak diaktifkan. Selain itu juga sistem menggunakan *proxy server* yang menggunakan *proxy squid*. *User* yang sudah terautentikasi pada sistem *RADIUS* akan di-*redirect* ke *proxy* oleh *firewall* yang terpasang pada *server RADIUS*. Cara kerja sistem, *user* melakukan koneksi dengan *access point* akan mendapatkan *ip DHCP* dari perangkat *access point* (*wireless hotspot*). Kemudian oleh *chillispot* yang tertanam di *access point* pengguna akan dialihkan ke halaman autentikasi untuk login sebelum menggunakan *internet* yang menggunakan protokol *https*. Setelah *user* mengisi *user* dan *password* akan diteruskan ke server *RADIUS* sebagai sistem autentikator. Sistem *RADIUS* ini menerapkan 3A; *authentication*: dimana saat *user* masuk akan diverifikasi pada data *user* yang tersimpan di database (*MySQL*), *authorization*: *user* yang berhasil *login* akan diperiksa otoritasnya sesuai yang ditentukan pada sistem, *accounting*: setiap transaksi dicatat oleh *freeradius* pada database *MySQL*.

Untuk pengujian penyerangan digunakan *attacker* yang menggunakan Sistem Operasi *Linux Backtrack 5r3*, tools yang digunakan antara lain *airmon, aircrack, tuxcat, macchanger, droidsheep, ComView*, dan lainnya.

B. Discovery

Fase *discovery* pada *penetration testing* ada dua bagian. Yang pertama merupakan awal *testing* sebenarnya, meliputi proses pengumpulan informasi dan *scanning*. Dari sini didapatkan informasi berupa *port*, *service* identifikasi, sistem operasi dari target. Pada fase ini dilakukan *scanning* untuk mengetahui informasi *access point*, klien yang terhubung ke *access point*, konfigurasi *access point* dan sistem seperti *DNS server*, dan lainnnya. Pada *fase scanning* ini merupakan penetrasi eksternal, penyerang belum melakukan autentikasi ke sistem *wireless*, akan tetapi sudah bisa terkoneksi ke *wireless* (karena sebagain besar sistem berbasis *RADIUS* ini merupakan sistem yang bersifat *open access,* setiap *client* langsung mendapatkan *IP* sebelum melakukan autentikasi).

- Informasi *Acess Point* : informasi SSID *access point*, *MAC address access point*, jenis enkripsi terlihat dengan tools *airodump* (pada penelitian ini tidak digunakan enkripsi jadi *access point* bersifat *open access*).
- Informasi *client* bisa didapatkan dengan menggunakan tool *airodump* dengan perintah berikut: bisa didapatkan informasi *client* yang terkoneksi ke *Access point*, *MAC address client*, dan jumlah paket *frame* dari *client*. (yang selanjutnya bisa dieksploitasi sebagai target).

```
airodump-ng -c 8 -a --bssid 68:7F:74:54:75:9C
mon0
```

- Untuk mengetahui *IP client* juga bisa menggunakan *tools network scanner* lainnya, mengingat akses jaringan *wireless* berbasis *RADIUS* server ini sebagian besar merupakan sistem *open access*, maka hal ini bisa dimanfaatkan oleh penyerang untuk melakukan *scanning* menggunakan *tools* seperti *nmap, armitage, tuxcut*, dan lainnya. Pada penelitian ini setelah mendapatkan *IP* dari *access point*. Peneliti melakukan *scanning* dengan menggunakan tools *nmap* yang ada di *armitage*, hasilnya didapatkan detail OS *client* yang terkoneksi ke AP selain *IP address*.
- Informasi *IP address router* (*access point*), beserta *DNS* bisa didapatkan setelah penyerang mendapatkan *IP address*. Dengan mengklik kanan *properties* jaringan (tergantung Sistem Operasi-nya), maka penyerang bisa melihat *IP router/gateway, DNS server* yang selanjutnya bisa dijadikan target penyerangan.
- Halaman autentikasi, pada saat pertamakali membuka *browser* dan memasukkan alamat, maka sistem akan me-*redirect* ke halaman autentikasi yang biasanya *URL*nya berupa *IP address* yang selanjutnya bisa dijadikan target penyerangan.

Setelah mendapatkan informasi pada awal tahapan *discovery*, maka tahap berikutnya adalah fase analisis celah keamanan, dengan data yang didapat dari tahap satu dilakukan pemetaan kerentanan (*vulnerability mapping*). Pada tahap ini, peneliti memetakan beberapa kemungkinan atau celah-celah yang bisa di penetrasi lebih lanjut berdasarkan informasi yang didapatkan pada sistem autentkasi *wireless* berbasis *RADIUS* yang diujicobakan. Pemetaan pentrasi untuk menguji celah keamanan yang bisa dilakukan adalah sebagai berikut: (a) Penetrasi pada *access point Hotspot*; (b) Penetrasi data *client* melalui *access point Hotspot*. (c) Penetrasi *User* autentikasi; (d) Penetrasi pada server *RADIUS Hotspot*.

C. Fase Penyerangan (Attack)

1) Penetrasi pada *Access point*.

Pada Penetrasi *Access point* dilakukan pengujian serangan *DoS (Denial of Services*), merupakan pengujian yang bersifat eksternal (pengguna belum terautentikasi). Sifat serangan bersifat aktif karena dampak serangan ini bisa mengganggu layanan jaringan *wireless*.

```
#cd /pentest/wireless/aircrack-
ng/scripts/airoscript-ng/src/plugins/
#echo 00:11:22:33:44:55 >blacklist
#mdk3 mon0 d -b blacklist -c Target_Channel
```

Sintak di atas berguna untuk menjalankan proses *DoS* menggunakan *tool mdk3*. Target penyerangan adalah Deautentifikasi *client* dari AP sehingga *client* tersebut tidak bisa teknoneksi ke jaringan *wireless*. Teknik *DoS* ini Membanjiri AP dengan permintaan AP authentifikasi, sehingga AP menjadi *overload*. Dampak dari serangan ini bukan hanya belaku bagi *access point* itu sendiri, tetapi berlaku juga bagi *client* yang menggunakan jaringan tersebut mengalami *disconnected* dengan layanan internet. Serangan ini akan berhasil jika *Access point* tidak dilengkapi dengan *firewall* untuk mencegah serangan *DoS*.

2) Penetrasi data client melalui Access Point Hotspot.

a) Session Hijacking

Untuk mengambil data *client* yang melewati *Access Point*, digunakan teknik *Session hijacking*, dalam teknik ini *attacker* mengambil kendali *session* milik *user* lain. *Session hijacking* ini merupakan jenis serangan pasif.

- *Client MAC address cloning*. Tujuan dari serangan ini adalah mencuri sesi *client* yang terkoneksi ke *access point* dengan merubah *MAC address* menjadi *MAC address client* yang terkoneksi. Serangan ini dilakukan sebelum autentikasi. Dengan menggunakan *tool airodump* bisa didapatkan informasi siapa saja yang terkoneksi ke *access point.*

```
#airodump-ng -c 8 -a -bssid 68:7F:74:54:75:9C mon0
```

Selanjutnya dengan menggunakan *tools TuxCut* dilakukan proses pemutusan *client* dan perubahan *MAC address* dan *IP* menjadi *MAC address* dan *IP client* target. Hasilnya koneksi *client* akan terputus dan penyerang bisa masuk dan bisa akses menggunakan internet tanpa melakukan login.

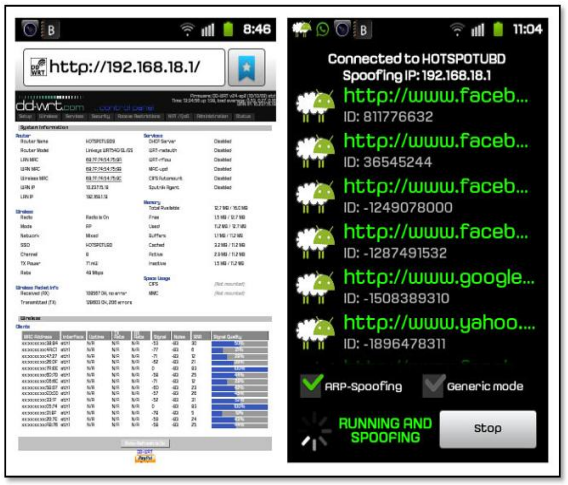
- *Sniffing Paket Menggunakan Ettercap*. Pada pengujian pertama dilakukan serangan pasif tanpa melakukan login. *Ettercap* merupakan salah satu tools yang banyak digunakan untuk melakukan kegiatan yang bersifat mengintip kegiatan *client* melalui jaringan (*sniffing*).

Proses *sniffing* paket *client* menggunakan *Ettercap* tidak berhasil karena yang terdeteksi hanya *DHCP Request* dari *IP Client*. Untuk proses *ARP Spoofing* yang dilakukan menggunakan tools ini mengakibatkan *flooding* di jaringan *wireless*, sehingga semua *client* yang terkoneksi terganggu.
Pada pengujian kedua dilakukan setelah autentikasi, kemudian di*sniffing* menggunakan *tools Ettercap*, yang terjadi paket *ARP spoofing* mengganggu jaringan dan paket *client* juga tidak bisa diperoleh.

- *Pengujian Tools Droidsheep pada SmartPhone Android*. *DroidSheep* merupakan aplikasi berbasis *Android* untuk menganalisis keamanan pada jaringan *wireless.* Dengan tools ini penyerang bisa melakukan *capturing* akses *facebook, twitter, linkedin* dan akses lainnya yang menggunakan protokol http [2]. Dengan *tools* ini dilakukan proses *ARP-Spoofing* kepada *access point*. Pengujian dilakukan dengan proses *sniffing* tanpa melakukan login autentikasi dan setelah autentikasi.

Untuk proses pengujian sebelum autentikasi stelah diujicoba beberapa kali didapatkan informasi mengenai situs yang diakses melalui *access point*, akan tetapi untuk *cookies* halaman yang diakses tidak berhasil di-*load*. Sedangkan pada pengujian *sniffing* setelah autentikasi, *cookies* untuk halaman *http* dari *client* berhasil didapatkan.

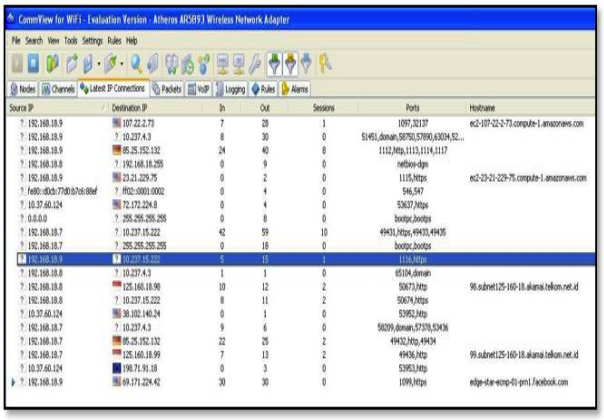
Pada pengujian didapatkan *client* yang ter-*sniffing* sedang membuka situs http://www.facebook.com. Dilakukan update status melalui *droidsheep* dengan memasukkan status "*Sniffing*" dan hasilnya langsung terlihat ter-*update*nya status akun facebook target. Jadi serangan ini termasuk ke dalam kategori *man-in-the-middle-attack*, dimana si penyerang bisa merubah informasi yang dia dapatkan.



Gambar 3. Tampilan port 80 dari *access point* dan proses ARP-Spoofing

- *Sniffing Menggunakan Tools CommView for WiFi*

Fungsi dari *software* ini berguna untuk memantau jaringan *wireless* 802.11 a/b/g/n. Baik itu berupa pemantauan dari aktifitas *client* sampai dengan jenis atau tipe *hardware* dari *access point* yang terdeteksi. Pengujian di sini bersifat eksternal (tanpa login), cukup mendapat *IP* dari AP dan selanjutnya melakukan penangkapan paket *client*, yang selanjutnya bisa dianalisis.



Gambar 4. Aktifitas dari *IP* yang terkoneksi ke AP

b) Evil Twin dan Access point MAC Spoofing.

Serangan lain yang diujicobakan pada infrastruktur *WLAN* adalah *Evil Twin*. Teknik *evil twin* ini membuat *access point* dengan *SSID* dan *channel* yang sama dengan *access point* target tetapi dengan *BSSID* (*MAC address*) yang berbeda dari *Access point*. Proses pembuatan *evil twin* ini bisa menggunakan *tools airbase*. Kemudian penyerang mem-*broadcast SSID evil Twin*. Pada saat yang sama dengan *tools aireplay* penyerang mengirim paket deautentikasi ke *access point* target dengan tujuan membuat target menjadi sibuk, dan koneksi client terputus sementara. Pada saat client terputus maka client akan berusaha untuk koneksi kembali ke *Access point* dengan *SSID* yang sama tanpa memperhatikan *BSSID access point*. *Client* akan terhubung ke *access point* fiktif. Setelah sambungan dibuat, penyerang dapat mengatur *aktifitas man-in-the-middle attack* dengan melakukan *sniffing*. *Attacker* bisa menangkap paket *client* dengan menggunakan mode monitoring pada *laptop attacker*, sehingga seluruh aktifitas *client* pada jaringan akan terdeteksi oleh *attacker* dan selanjutnya menggabungkan teknik-teknik yang lain untuk melakukan penyerangan pada target

3) Penetrasi User Autentikasi.

Pada pengujian ini sistem autentikasi *wireless* berbasis *RADIUS* server yang diuji menggunakan halaman login autentikasi yang *hotspotlogin.php* yang dikembangkan dari http://sourceforge.net/projects/ezradius. Halaman autentikasi diletakkan pada server *RADIUS*, dan diaktifkan fitur *https*,

sehingga pada saat pertama kali *user* melakukan login akan di-*redirect* ke halaman https. Pada pengujian ini dilakukan pengujian menggunakan teknik *SQL injection* dan *cross side scripting*.

a) SQL Ijection.

SQL Injection merupakan aksi *hacking* yang dilakukan di aplikasi *client* dengan cara memodifikasi perintah atau sintak *SQL*. Pada pengujian dicoba dengan menggunakan berebagai variasi *query*, pada portal web autentikasi *wireless RADIUS Hotspot* dengan sintak *SQL* pada halaman *hotspotlogin.php*. Hasil pengujian ini sangat tergantung pada *script* halaman autentikasi dan konfigurasi server web, karena celah keamanan ini bisa dimanfaatkan pada server web yang tidak dikonfigurasi dengan baik dan *script* yang lemah. Pada pengujian di sini setelah dicoba berbagai *query injection* dan tidak memperoleh hasil.

b) XSS (Cross-Site Scripting)

Teknik ini dilakukan dengan cara menginjeksi atau memasukkan *script* ke dalam website melalui *browser*. Aksi *XSS* ini memanfaatkan metode *HTTP GET/HTTP POST*. Pada pengujian *script XSS* dicobakan pada portal auntentikasi untuk mengetahui apakah portal tersebut bisa di *XSS* atau tidak. Hasilnya target tidak bisa di XSS dan tidak bisa di-*redirect* ke halaman lain. Karena halaman portal secara default selalu meredirect ke *port 3990* yang digunakan *chillispot*.

4) Penetrasi pada server RADIUS Hotspot.

Pada pengujian pada server *RADIUS Hotspot*, dilakukan proses *scanning* menggunakan *tools nmap*, hasilnya tergantung pada konfigurasi sistem server. Pada proses *scanning* didapatkan hasil *port* yang terbuka. Hasil *scanning* digunakan penyerang untuk melakukan penetrasi lebih lanjut ke sistem. Pengujian lain yang dilakukan adalah melakukan proses *DoS* ke server *RADIUS*. Hasil yang didapatkan tergantung dari konfigurasi server itu sendiri.

D. Fase Reporting

Dari hasil pengujian yang didapatkan dibuat laporannya serta rekomendasi untuk perbaikan celah keamanan pada sistem autentikasi berbasis *RADIUS*.

TABLE I. HASIL PENETRASI

No	Serangan	Tools	Keterangan	Hasil
1	Penetrasi pada AP	*mdk3*	Pengujian Eksternal tanpa login	Berhasil melumpuhkan AP
2	Penetrasi data *Client* pada AP			
	a. *Client MAC address cloning*	*Airodump, TuxCut*	*Session hijacking*, merupakan serangan pasif tanpa login.	Koneksi *client* putus dan diambil alih, serta bisa meng-*capture* paket *client*.
	b. *Sniffing* Paket dengan *tools Etercap*	*ettercap*	Serangan aktif yang dilakukan tanpa login dan sesudah login	Hanya berhasil melihat *IP client* yang terkoneksi ke AP. Dampaknya mengganggu aktifitas jaringan *wireless*.
	c. *Sniffing* paket dengan *tools droidsheep*	*droidsheep*	Serangan pasif, dilakukan dengan login dan tanpa login	Berhasil menangkap paket http dari pengguna AP. Jika dilakukan setelah login bisa melakukan *man-in-the-middle-attack* untuk akses *facebook*, dll (protokol http)
	d. *Sniffing* menggunakan *ComView*	*ComView*	Serangan pasif tanpa login	Bisa menangkap paket *client* di sekitar *wireless*
	Evil Twin & Access point MAC Spoofing	*Airbase, Tuxcut*	Serangan pasif	Bisa memperdaya korban untuk melakukan koneksi ke AP palsu.
3	Penetrasi *User* Autentikasi			
.	*SQL Injection & Cross-Site Scripting*	-	Serangan pasif tanpa login	Hasil Tergantung kelemahan *script* autentikasi dan konfigurasi server
4	Penetrasi Ke Server *RADIUS*	*Nmap, denial, smurf, hping*	Serangan pasif dan aktif setelah login	Tergantung konfigurasi server dan *firewall*

Jika dilihat dari hasil penetrasi yang dilakukan, terlihat sistem autentikasi berbasis radius memiliki celah keamanan yang bisa dimanfaatkan penyerang antara lain untuk melumpuhkan layanan *wireless* yang disediakan, dan celah lain yang paling berbahaya yaitu celah *sniffing* data client yang menggunakan layanan tersebut. Tidak amannya sistem tersebut terutama dikarenakan koneksi antara *supplicant* (*client*) dan *authenticator* (*access point*) yang tidak terenkripsi.

IV. REKOMENDASI PENGAMANAN

Dari beberapa celah keamanan yang didapatkan pada pengujian yang sudah dilakukan maka untuk menutup celah keamanan sistem autentikasi *wireless* berbasis *RADIUS* bisa diberikan solusi sebagai berikut:

- Sistem autentikasi *wireless* berbasis *RADIUS* tidak bisa hanya mengandalkan proses autentikasi sebagai pengamanan. Celah yang paling besar pada sistem tersebut adalah karena penyerang langsung bisa terkoneksi ke *Access point* dan mendapatkan *IP address* sebelum melakukan autentikasi. Hal ini dikarenakan administrator mengutamakan sisi kemudahan layanan. Akan tetapi resiko dari celah ini dari pengujian

penyerang bisa melakukan penetrasi *DoS* ke AP, melakukan *sniffing* paket, dan mencoba melakukan penetrasi *user* autentikasi. Untuk itu bisa digunakan alternatif penggunaan *EAP-TLS* yang dikombinasikan dengan *RADIUS*. Sehingga *user* yang bisa terkoneksi adalah *user* yang sudah men-*download* sertifikat *TLS* pada komputernya. *EAP-TLS* meng-*generate dynamic WEP (shared secret)* setelah proses pertukaran, sehingga *supplicant* dan *authenticator* dapat melakukan komunikasi yang aman berdasarkan *per-packet authenticated* [5]. Dengan demikian paket yang dikirim dari *supplicant (client)* ke *autenthicator (access point)* akan terenkripsi, sehingga mengatasi celah keamanan *session hijacking* dan *sniffing* paket.

Demikian juga untuk *sniffing* paket yang menggunakan *IP* dan *MAC address clonning*. Si penyerang tidak bisa melakukan *scanning client* dan mendapatkan *IP address* jika tidak memiliki sertfikat digital pada komputernya. Pada kasus si penyerang melakukan perubahan *IP* dan *MAC address* dengan mengintip *IP* dan *MAC address* secara manual pun tidak akan bisa memutuskan koneksi *client* ke *access point*, karena dengan sertifikat digital *EAP-TLS* akan menggenerate *WEP* dinamis.

EAP-TLS juga merupakan solusi dari teknik *evil-twin* dan *MAC address* spoofing, karena meskipun si penyerang menggunakan AP plasu yang mirip dengan AP target yang ada, *fake* AP tersebut tidak memiliki sertifikat digital yang di-*generate* oleh *TLS* sehingga *client* akan tahu jika ada perubahan AP. Di Sistem operasi akan memberikan pesan adanya ketidaksamaan sertifikat yang dimiliki.

- Untuk menutup celah keamanan *Access point* dari serangan *DoS* maka di *Access point* bisa dipasang *firewall* untuk mencegah *DoS* (tergantung jenis *Access point* dan *firmware*). Pada penelitian ini menggunakan *firmware DDWRT* dan *firewall* yang bisa digunakan untuk mencegah teknik *DOS* ini bisa digunakan contoh berikut [4]:

```
## SYN-FLOODING PROTECTION
# Rule firewall ini membatasi incoming connections.
Paket dibatasi
1/limit tiap detik. Pada kasus ini 4 connections
dalam satu detik.

IPtables -N syn-flood
IPtables -A INPUT -i $IFACE -p tcp --syn -j syn-flood
IPtables -A syn-flood -m limit --limit 1/s --limit-
burst 4 -j RETURN
IPtables -A syn-flood -j DROP

## Firewall ini memastikan NEW tcp connections
merupakan SYN packets
IPtables -A INPUT -i $IFACE -p tcp ! --syn -m state -
-state NEW -j DROP
```

- Untuk pengamanan serangan yang memutuskan koneksi *client* menggunakan *Software TuxCut* atau sejenisnya bisa diatasi dengan menggunakan *software AntiTuxCut* atau *NetCut Defender*. Demkian juga untuk menghindari *tools session hijacking* seperti *droidsheep* dan sejenisnya maka pengguna bisa menggunakan *tools* seperti *droidsheep guard*, yang mencegah adanya *sniffing* paket *session hijacking*. Selain itu juga sebisa mungkin untuk akun-akun seperti *facebook, twitter, email*, dan lain-lain sebisa mungkin menggunakan protokol *http*.

- Untuk menutup celah keamanan penetrasi *user* autentikasi dengan *SQL injection* dan *cross side scripting*, maka perlu dilakukan audit seperti menggunakan *tools web vulnerability scanner, nikto*, dan lainnya untuk tahu celah keamanan. Jika ditemukan maka diperlukan perbaikan *script* dan konfigurasi sistem seperti menggunakan protool *https*, menutup akses direktori dengan mengaktifkan fitur *.htaccess* dan *.htpasswd*. Sehingga untuk mengakses direktori yang digunakan untuk web server autentikasi memerlukan *password*. Selain itu juga fitur direktori list juga dinon aktifkan di konfigurasi webserver.

- Untuk pengamanan server *RADIUS* yang bisa dilakukan adalah selalu melakukan *patching system*, memasang *firewall* untuk mencegah *DoS*, dan jika perlu gunakan *portsentry* dan IDS untuk menggagalkan aksi *scanning* dan penyerangan yang dilakukan penyerang.

V. KESIMPULAN DAN SARAN

Dari hasil penelitian dan pengujian keamanan yang dilakukan ditarik beberapa kesimpulan :

a. Sistem autentikasi *wireless* berbasis *RADIUS* masih memiliki beberapa celah keamanan yang bisa dimanfaatkan oleh *hacker*. Celah keamanan itu berupa kemungkinan serangan *DoS* ke *Access point*, Pencurian data *client* menggunakan *session hijacking*, dan pemutusan koneksi *client* yang sedang terkoneksi untuk mengambil alih sesi koneksi, serta eksploitasi serangan ke server. Selain itu karena koneksi autentikasi *wireless* berbasis *RADIUS* merupakan sistem yang bersifat open akses maka si *hacker* bisa mengeksploitasi serangan ke *access point*, halaman autentikasi, server *RADIUS* tanpa perlu melakukan login.

b. Penetrasi jaringan sangat dibutuhkan untuk mengetahui celah keamanan sistem dan jaringan. Hasil penetrasi testing bisa digunakan untuk perbaikan sistem ke depan.

c. Untuk perbaikan sistem autentikasi *wireless* berbasis *RADIUS* maka sebaiknya sistem dikembangkan menjadi sistem berbasis *EAP-TLS over RADIUS*. Selain itu juga penggunaan *firewall* pada *Access point*, dan server *RADIUS* serta pengamanan lain bagi server sangat dibutuhkan untuk menjaga ketersediaan layanan jaringan *wireless*.

REFERENSI

[1] A. Supriyanto, "Analisis kelemahan keamanan pada jaringan wireless," Jurnal Teknologi Informasi DINAMIK Volume XI, No. 1, Januari 2006 : 38-46.

[2] http://droidsheep.de

[3] http://idsirtii.or.id/trafik-bulanan

[4] http://www.sns.ias.edu/~jns/files/iptables_ruleset

[5] H. Onder, " Session hijacking attacks in wireless local area networks," Master of Science in Computer Science. Naval postgraduate school, 2004.

[6] K. Scarfone, M. Souppaya, A. Cody, A.ngela Orebaugh, “Technical guide to information security testing and assesment, “ Recomendations of the National Standard and Technology. NIST Special Publicaton 800-115, 2008.

[7] R.M. Davison, M.G.Martinsons, N. Kock, “Principles of canonical action research”, Journal: Information Systems Journal: 14, 65–86, 2004.

[8] S. Ali, T. Heriyanto, “BackTrack 4: assuring Security by Penetration Testing.” Packt Publishing, 2011.

[9] Sugiyono, “Memahami penelitian kualitatif.” Alfabeta: Bandung, 2005.

[10] Y.N. Kunang, I.Z. Yadi., “Autentikasi pengguna wireless LAN berbasis Radius server (studi kasus: WLAN Universitas Bina Darma).” Jurnal Ilmiah Matrik, Vol. 10 No. 2, Agustus 2008.